**Some Home-User Data Security Basics**

Although the recent malware attacks on important Alaska governmental departments such as health and human services, courts, and school districts have received a great deal of attention, human error causes the large majority of serious data security breaches and operational disruption.

But, there's a lot that you can do to reduce your risks. Most malware attacks are sprayed broadly across the Internet, not specifically targeted.

Malware threats are evolving very rapidly, so a short refresher course in avoiding human error is always in order for all of us. The human error avoidance training at [www.KnowBe4.com](http://www.KnowBe4.com) is generally considered one of the better online resources and should be reviewed periodically. It may save you serious grief.

Still, no one's perfect and threat vectors are becoming so sophisticated that discerning the real from the fake taxes even the experts. As then FBI Director Robert Mueller famously warned about seven years ago, it's not IF your systems become infected, but WHEN. To that, I would add: "..and how severely".

In many ways, data security is in tension with the easy 24/7/365/anywhere data accessibility that’s now so prized by highly mobile lawyers. The risks and serious consequences of data breach may have reached the point of over-riding our accustomed easy connectivity.

The thoughts below are primarily focused upon the everyday person rather than larger groups with IT people.

So, let’s consider some reasonably achievable aspects of hardening your online environment to the extent that it remains connected. Trying to do everything at once is a recipe for chaos and oversights, so we recommend improving your data security in a planned, orderly way over several months,

Security Software

* It’s important to remember that many threats are sprayed broadly across the Internet, often using millions of stolen Email addresses or phone numbers at a time. These are just as damaging as a specifically targeted one. Specifically targeted threats happen but are less common.
* You’ll need a comprehensive real-time security suite for every end-point computer and smartphone. Android smartphones are considered to be more vulnerable than iPhones. The District is providing protection for one device used by Rotarians with admin level access. You may need to personally get your own account and buy protection for extra devices if you use several, such as more than one computer plus your smartphone, etc.
* Most security suites now protect multiple devices for a single annual fee. No single security suite is perfect and most have differing, overlapping competences.
* Free security software is definitely not an adequate defense by itself.
* Bitdefender is currently considered one of the best. The security suite should run at all times on every endpoint computer and device.
* You’ll need to run both anti-virus scanning AND real time protection, not just one or the other. While traditional anti-virus scans are useful, they don’t provide any protection against immediate attacks – by the time that malware is detected by an occasional virus scan, it’s probably already done its damage and stolen your data.
* Always run VPN (Virtual Private Network) software as well. It provides an additional level of protection for your Email and other communications without getting in the way.
* You can use the free version of some security software in a complementary fashion. For example, if you use BitDefender as your regular paid full-time security software, then you can periodically run manual scans of your devices with the free, well-regarded Malwarebytes security software.

Operating Systems

* Use a current operating system that’s updated regularly by the vendor. Windows 8 software is the oldest Windows version that still supported and updated. Windows 7 users are more vulnerable because that software no longer receives protective security updates. Once support ends for an operating system, it’s time for you to move on. Immediately.
* Enable automatic updating with daily update checking. BitDefender includes an easy to use “Vulnerability Scan” that checks everything, including operating system updates, and suggests corrective action to protect you and your data.
* Enable newer security add-ons, such as the newly enhanced Windows Defender, but don’t rely upon them too much. They’re simply an extra layer of armor plate, but no armor plate made will stop every round.
* Turn off Remote Access functions.
* Enable Data Execution Prevention.
* Regularly create a System Restore Point.
* Go through every Windows applet and manually turn off their sound and video functions unless you use them regularly. You’ll be amazed at how many there are and the default is sound and video-enabled. These have become a favored approach to breaching your privacy.
* Remotely accessible voice monitoring like Alexa are a major security threat.
* Be cautious using wireless Internet access – at a minimum, use VPN software whenever connecting wirelessly to the Internet.

There’s a lot here, but it’s still easier in the long term than the nightmare of a data security breach.